



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/905,113	07/16/2001	Scott A. Vanstone	06944.0044	3558
27155	7590	10/18/2005	EXAMINER	
MCCARTHY TETRAULT LLP BOX 48, SUITE 4700, 66WELLINGTON STREET WEST TORONTO, ON M5K 1E6 CANADA			CALLAHAN, PAUL E	
			ART UNIT	PAPER NUMBER
			2137	

DATE MAILED: 10/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/905,113

Applicant(s)

VANSTONE, SCOTT A.

Examiner

Paul Callahan

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 27 May 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-12 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-12 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 16 July 2001 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)

~~Paper No(s)/Mail Date~~ P.C.

- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

Response to Amendment

1. Claims 1-12 are pending in this application and have been examined.

Specification

2. The amendment filed 5-27-2005 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows:

On page 2 of the Amendment, first paragraph, the new matter is added by virtue of the following passage: "The secure module can be adapted to be removably coupled to the personalized device." This feature was not previously disclosed.

Applicant is required to cancel the new matter in the reply to this Office Action.

3. The amended title is acceptable.
4. The disclosure is objected to because of the following informalities: It is not clear what reference number 30 is. On page 6 line 24, and on page 7 line 18 reference number 30 is designated as a display, but on page 6 line 38 it is designated as a secure path.

Claim Objections

5. Claim 12 is objected to because of the following informalities: The specification does not teach that the secure module is adapted to be "removably coupled to said personalized device." Appropriate correction is required.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1,2,4-12 are rejected under 35 U.S.C. 102(b) as being anticipated by Wang US 5,917,913.

As for Claim 1, Wang teaches a method of verifying data integrity between at least two correspondents in a public-key cryptographic scheme, at least one of said at least two correspondents having a main processor and a secure module, said secure module being independent of said main processor's control, said method comprising the steps of: assembling data on at least one of said at least two correspondents (col.4 lines 12-17); displaying data under control of said main processor to produce a first output (col.4 lines 17-21, col.2 lines 18-23), forwarding said data to said secure module and displaying said data from said secure module to produce a second output to permit

Art Unit: 2137

a comparison of said first and second outputs (col.4 lines 41-44, col.10 line 66 thru col. 1 line 5), comparing said first output and second output (col.6 lines 35-48), instructing said secure module to generate a signature upon a favorable comparison of said first output and said second output (col.4 lines 44-50, col.5 lines 50- 67), and whereby said favorable comparison indicates data integrity such that said at least one of said correspondents signs said data (col.4 lines 44-50, col.5 lines 50-67).

As for Claim 2, Wang teaches at least one of said at least two correspondents is a personalized device (col.4 lines 8-12).

As for Claim 4, Wang teaches said personalized device is a personal digital assistant (col.4 lines 8-12).

As for Claim 5, Wang teaches said favorable comparison is characterized in that said first output and said second output are logically related to one another (col.6 lines 36-48).

As for Claim 6, Wang teaches said logical relationship is such that said first output and said output are identical (col.6 lines 36-48).

As for Claim 7, Wang teaches said step of displaying said data message

Art Unit: 2137

includes displaying a portion of said data message (col.4 lines 41-44., col.10 line 66 thru col.11 line 5).

As for Claim 8, Wang teaches said favorable comparison is characterized in that a portion of said first output and a portion of said second output are logically related to one another (col.6 lines 36-48).

As for Claim 9, Wang teaches said logical relationship is such that said portion of said first output is identical to said portion of said second output (col.6 lines 36-48).

As for Claim 10, Wang teaches a method of establishing a secure communication path for data between a personalized device and an user of said device in a cryptographic scheme, said device having a main processor and a secure module independently operative of said main processor, said method comprising the steps of: providing an interface between said device and said user, said interface having an input device and an output device for providing a means for interaction between said user and device, said input device and output device controllable by said main processor (col.10. line 55 thru col-11 line 5), providing a secure communication path between said secure module and a secure input device and a secure output device coupled thereto, said secure path logically isolated from any other communication path (col.6 lines 55-67), assembling data at said input device and said secure input device and forwarding said data to said

Art Unit: 2137

secure module over said trusted communication path (col.4 lines 41-44, col.10 line 66 thru col. 11 line 5) and displaying said data on said output device and said secure output device to permit comparing said data displayed on said output device and said secure output device (col.6 lines 36-48), whereby said user of said personalized device can determine said integrity of said data based on said comparison (col.5 lines 18-21 ; col.5 lines 51-64., col.6 lines 36-48).

As for Claim 11, Wang teaches said user actuates said secure input device based only on said output of said output device (col.6 lines 36-48).

As for Claim 12, Wang teaches a method for verifying the integrity of a data message between a correspondent and a personalized device in a communication system, each correspondent adapted to receive and transmit data messages, said method comprising: containing a secret key in said secure module, said secure module adapted to be removably coupled to said personalized device and communicatively coupled thereto (col.5 lines 1-9), and controlling access to said personalized device based on a comparison of data from said secure module and data from a main processor of said personalized device, said main processor independently operable of said secure module (col. 1 lines 35-67).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wang, and further in view of Vatanen WO 00/54457. Wang teaches the method of claim 2 but does not teach said personalized device is a mobile phone. Vatanen teaches said personalized device is a mobile phone (fig. 1, page 7 lines 15-36). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Wang's portable electronic device with Vatanen's telecommunication system in order to implement a secure method for conducting transactions within a mobile telecommunication system (page 2 line 19 thru page 3 line 28).

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The following US Patent Document teaches features pertinent to the Applicant's disclosure.

Rosen 5,557,518

Art Unit: 2137

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Emmanuel Moise, can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is: (571) 273-8300


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

8-3-05

